

# A Reality Check on a Cyber Force

*Col Corey M. Ramsby, USAF*

*Panayotis A. Yannakogeorgos*

## Abstract

It is premature to call for a separate cyberspace armed service, independent of the other services and agencies, to project power and protect vital US national security and economic vitality interests. There are four key prerequisites before achieving this goal: 1) a unique, strategic military capability unachievable by any of the other services and agencies; 2) corresponding technological advances; 3) an unrestricted battlespace; and 4) political champions to maneuver the bureaucracy and pass legislation.



Today, the Internet has become a key enabler of wealth generation, economic revival, human development, and poverty alleviation. Developed societies as a whole depend on cyberspace equities to prosper, and access to the domain is a requirement for developing countries to move toward prosperity.

The world is dependent upon a new domain that is ambiguously defined and for which national security implications are only now beginning to be cogently understood by senior leaders around the world.

Concurrent with this dependence is the presence of malicious actors who erode security and trust by exploiting technical vulnerabilities and human complacency that enables espionage, crime, and nation-state aggression. Thus, economic vitality is held at risk, and the national security apparatus is struggling to determine how to move from insecurity as the

---

Col Corey M. Ramsby is director of staff, Curtis E. LeMay Center for Doctrine Development and Education. He is a graduate of the Air War College, Air Command and Staff College, and Purdue University. Colonel Ramsby served on the Air Staff and Joint Staff and completed multiple deployments to Afghanistan during Operation Enduring Freedom.

Pano Yannakogeorgos is a research professor of cyber policy and global affairs at the Air Force Research Institute. His research interests include the intersection of cyberspace and global security. He holds PhD and MS degrees in global affairs from Rutgers University and an ALB degree in philosophy from Harvard University.

norm to a domain of human activity wherein trust, security, and sovereign control of malicious activities reign.

To address aspects of the national security implications of cyberspace, the Department of Defense (DOD) has identified cyberspace in military strategy and doctrine as an operational domain in which to organize, train, and equip forces to ensure it has the necessary capabilities to operate effectively across all operational domains of warfare.<sup>1</sup> With this designation comes significant implications that include defending, exploiting, sustaining, and evolving capabilities in pursuit of national objectives. The designation of cyberspace as an operational military domain also brings with it a debate about how to structure US military assets to realize their full potential and whether the current military construct can support its maximum development. This debate is framed around two questions. Can the current DOD establishment meet the demands, obligations, and future requirements of the cyberspace domain? Or, is a separate force, independent of the other services and agencies, needed to project and protect vital US cyberspace interests?<sup>2</sup>

In a January 2014 *Proceedings* magazine article, “Time for a US Cyber Force,” Adm James Stavridis, US Navy, retired, and National Security Agency (NSA) planner David Weinstein draw strong parallels to Brig Gen William “Billy” Mitchell, US Army, and his quest for a separate US Air Force (USAF) following World War I. They call for a separate and independent cyber force to fully develop, defend, and exploit America’s newest war-fighting domain.<sup>3</sup> Using Mitchell’s argument as the historical context, they recommend we learn from history to avoid the bitter debates of why and how cyberspace should be managed and to realize that a new contested domain requires a separate force free from the other services’ internal influences, biases, and priorities. In their words, “We are once again at the beach at Kitty Hawk, . . . [and] let’s not wait 20 years to realize it.”<sup>4</sup>

Stavridis maintained this position in December 2015 before the Senate Armed Services Committee. In his testimony he continued to advocate for a separate cyber force, highlighting that “the sooner we have not only a cyber command, but, in my view, a cyber force—small, capable—I think we would be well served.”<sup>5</sup> Similar viewpoints have been recounted by other officials, including Secretary of Defense Ashton Carter, who indicated that a separate cyber force is one possible future for the DOD.<sup>6</sup> However, it is premature to consider a separate cyberspace

force independent of the other services for several reasons. We believe four particular criteria should be met before creating a separate armed cyberspace service. These include a unique, strategic military capability unachievable by any of the other services or agencies; corresponding technological advances; an unrestricted battlespace to develop, test, and refine theories, weapons, and tactics of cyberpower; and political advocates who can maneuver the bureaucratic and legislative terrain needed to create a separate military service. This is not to say these are the only criterion, rather that without them the case for an independent cyberspace force lacks sufficient rationale. We further conclude that instead of a new cyber force, a new cyberspace *agency* be optimally designed, free from the other services' internal influences, biases, and priorities, to compete within the current threat environment until the criteria for creating a separate cyber force are met.

It is not the purpose here to outline why or how a separate force can or cannot be established. Instead, we analyze the parallels being drawn between how the USAF was created and the proposed formation of a separate US Cyber Force. Specifically, we focus on the 20 years of airpower development and debate Stavridis and Weinstein would prefer we avoid. The debate for a separate cyber force should not center on whether the cyberspace arm is subservient to the other services in a manner similar to the air force debate. Rather, it should focus on whether or not a separate branch of the armed services could match and exceed existing services' and agencies' capabilities without degrading core missions and at a resource savings that can overshadow the disruption and overhead costs of establishing a new military branch.

For the air domain, the unique capability developed into strategic bombing and the capacity to strike an adversary's homeland without the need for land invasions or sea battles.<sup>7</sup> The technological advancement that realized the capability was the long-range bomber, such as the B-29, and delivery of atomic weapons.<sup>8</sup> The unrestricted battlespace was the European and Pacific strategic bombing campaigns of World War II. The leadership and proponents for a separate air arm included senior leaders such as presidents Franklin Roosevelt and Harry Truman; Army generals Dwight Eisenhower, George Marshall, and Henry "Hap" Arnold; and Assistant Secretary of War for Air Robert A. Lovett, among others. This is not to say these were the only criterion. Rather, without

them the case for an independent air force would have certainly lacked rationale, and the same applies to cyberspace today.

### **A Distinct Strategic Capability**

Because the missions of the services and the combat support agencies are so ingrained and dependent on cyberspace, the first criterion to be met in the discussion of a separate cyber force is that of a distinct strategic capability unique enough that only a separate service could provide it. Otherwise, a separate cyber force would require a profound cost-benefit analysis so monumental in savings and mission advancement the services and agencies could not refute, dispute, or refuse its potential. At the present, neither exists. If the former did exist, would we know what it looked like? Chief of Staff of the Air Force Gen Mark Welsh III provided a potential view during his Air Force Update speech in September 2014.

General Welsh stated the USAF needs “an air component commander capability to sit in the Air Operations Center when the big fight starts, hit the cyber easy button and watch the enemy RPAs (remotely piloted aircraft) pool at his feet. Or when the enemy starts to shoot missiles toward friendly forces, employ a tool that allows these missiles to sit and sizzle on the pad or go half way, turn around, and go home.”<sup>9</sup> He followed the comment with the question of who might be working the solution and how it could be expanded “in a big way.” Meant to be forward leaning and thought provoking, Welsh’s comments fortuitously highlight two existing aspects of cyberspace: cyberspace power theories are primitive but evolving and, much like the early theories of airpower, can be perceived as a panacea above existing weapon capabilities and strategy.

These perceptions seem reminiscent of the interwar air power theories developed by Giulio Douhet and Mitchell. David MacIsaac provides a treasure trove of intellectual analysis on early airpower theories in his influential essay “Voices from the Central Blue: The Air Power Theorists.”<sup>10</sup> One of MacIsaac’s more interesting cogitations is the vision that airpower “invariably outran the reality of the moment” clouding the debate with disappointment and derision based on aspirations that airpower could “provide quick, clean, mechanical, and impersonal solutions to problems which others had struggled for centuries.”<sup>11</sup> The “cyber easy button” proposed by General Welsh bears a similar resemblance and therein lies a strategic paradox: the vision of a great capability beyond the means of

the services but dependent on them to develop it. Douhet and Mitchell well understood this paradox and the reliance on biased army and naval officials to advance airpower's role, strategy, doctrine, and capabilities.

Though for dissimilar reasons, both theorists surmised airpower could not reach its potential while dependent on another service for its development. Douhet called for an "independent air force armed with long-range bombardment aircraft," while Mitchell, less concerned of the particular delivery vehicle, focused on "centralized coordination under the control of autonomous air force command."<sup>12</sup> During their time, both men's ideas eclipsed the strategic utility of the air domain and the airplane remained deferential to land and naval forces.

Today, each of the armed services and several government agencies currently have significant equity in the cyberspace mission. The 2014 *Quadrennial Defense Review* entrenches this commitment on the part of the DOD with the requirement for cyber mission forces sourced via the services.<sup>13</sup> Additionally, the DOD includes the NSA and Defense Information Systems Agency, the missions of which heavily reside in the cyberspace domain and in most cases outpace the services' capacities and capabilities. Cyberspace visions appear on a similar track. Evolving cyberspace capabilities exist but rely on the services and support agencies for their development and thus remain constrained by each accordingly. Additionally, cyberspace maneuvers are largely tactical, precisely targeted, and/or so shrouded in secrecy that they remain useless to the public debate of establishing a separate cyberspace force. Separate military services are not created based on threat alone. Thus, creation of a separate cyberspace force is unlikely to precede the development of a unique strategic cyberspace capability.

## Corresponding Technological Advances

The theory of strategic bombing required technological advancements and weapon systems to progress from thought and debate to reality. Long-range bombers, advanced bomb sights, and atomic weapons all contributed to its evolution. Strategic cyberspace development must include similar technological advancements, whether they are software, hardware, or human presence in the battlespace.

Again, looking at the path to USAF independence, the long-range bomber underpinned the ambition and premise for service equality. The ability to attack an enemy's heartland without a land invasion funda-

mentally changed America's strategic approach to war, and the role of the B-29 Superfortress cannot be overstated in this regard. Considered the "greatest gamble of the war," the \$3 billion development and subsequent deployment of the B-29 to the Pacific theater in 1944 marked the point where air-domain technology converged with interwar theory and propelled airpower into an independent, rather than a complementary, role in World War II.<sup>14</sup> Commanded by General Arnold and the Joint Chiefs of Staff in Washington, DC, the B-29s were organized under the Twentieth Air Force and remained autonomous from the three Pacific theater commanders: Adm Chester Nimitz, Gen Douglas MacArthur, and Gen Joseph Stilwell.<sup>15</sup>

To put the strategic impacts of the B-29 into perspective, "with high explosives alone, the Twentieth Air Force levelled 2,333,000 homes in Japan, and most of the business and industry in sixty cities."<sup>16</sup> The conventional bombing campaign killed "at least 240,000 and wounded more than 300,000."<sup>17</sup> During March through June 1945 alone, Japanese deaths reached 127,000 in its six largest cities.<sup>18</sup> By any measure, the devastation provided by the B-29 produced strategic options and effects not seen prior to its arrival in the Pacific. Coupled with the atomic bomb, the B-29 provided President Truman with a one plane, one crew, one bomb, one city capability that destroyed Hiroshima and Nagasaki, forcing Japan's unconditional surrender while avoiding a difficult and costly land invasion. In his words, airpower had developed to a point "equal to those of land and sea power," and its contributions to strategic planning were as great.<sup>19</sup>

Technological advances in cyberspace pale in comparison with regards to the overall devastation and political impact of airpower. There are various flavors of digital intelligence tools and disruptive techniques, with the most sophisticated employing multiple, previously unknown (zero-day) vulnerabilities against software code and some using trusted hardware vendor certificates to cloak their presence. The standard bearer of such advanced techniques is the precision-guided malicious software (malware) Stuxnet. The code, so precisely written, activated only after verifying it was indeed in the Natanz nuclear facility's internal network by comparing the exact size and number of centrifuges operating in the facility. Stuxnet has been tagged as the first specifically designed cyber weapon ever deployed.<sup>20</sup>

Stuxnet certainly created in the mainstream an awareness of the interdependence between physical platforms and the ability of software to trigger effects in cyber control systems to produce effects in the physical world. Exaggerated claims that see parallels between malicious software and the use of atomic weapons assert that this cyber-enabled tool is something new in history.<sup>21</sup> Stuxnet set the Iranian nuclear enrichment program back months to years and accomplished what was previously only militarily possible via kinetic means. As has been documented, the technical sophistication of the malware is evidence of a team that had “the detailed pin-point manipulations of these sub-controllers indicate a deep physical and functional knowledge of the target environment; whoever provided the required intelligence may as well know the favorite pizza toppings of the local head of engineering.”<sup>22</sup> Further, it has been noted that Stuxnet programmers were “in a position where they could have broken the victim’s neck, but they chose continuous periodical choking instead. Stuxnet is a low-yield weapon with the overall intention to reduce the lifetime of Iran’s centrifuges and make their fancy control systems appear beyond their understanding.”<sup>23</sup> That the programmers chose not to resort to more drastic measures, demonstrates intent to disrupt the data flows on which humans relied on to ensure the proper functioning of the centrifuges. The result was damaged centrifuges and a delayed nuclear program rather than the destruction of the nuclear centrifuges on a scale of a bombardment that might cross the use-of-force threshold. Hence, Stuxnet appears as a software tool enabling sanctions enforcement.

The challenge with Stuxnet—and other similar cyber weapons—is that discovery leads to obsolescence because the designs can be unlocked by anyone with the skill set to reverse engineer them. Additionally, secrecy and nonattribution prevail as essential aspects in their development and deployment. These factors highlight the juvenescent state of the cyberspace battlefield, prevailing technologies, and the current abilities of the services and combat support agencies to meet national requirements. Therefore, the impact of creating a separate cyberspace service has not reached a point technologically where the benefits can outweigh the costs to the current service and agency structure. That is not to say cyberspace is uncontested or the United States is not dangerously vulnerable. Rather, the risk-benefit analysis, especially with the standup of US Cyber Command (USCYBERCOM) and the cyber mission forces,

remains in favor of the current military service construct shaded by the culture of secrecy in the intelligence community.

## **An Unrestricted Battlespace**

More than 45 years after researchers at the University of California–Los Angeles first connected to a computer at Stanford University and two decades since the explosive Internet expansion of the early 1990s, global interconnectedness has literally changed the political and social fabrics of every developed and developing nation. Today, societies rely on elements of cyberspace for commerce, education, social networking, and control of public utilities. This interconnectedness has fundamentally shifted the way nations and societies conduct and resolve conflict because it provides a level of engagement, good or bad, at speeds and depths not previously known. Malicious cyber actors exploit vulnerabilities in these digital systems and pose “a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The malicious cyber-enabled activity must have the purpose or effect of significantly harming or compromising critical infrastructure; misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.”<sup>24</sup> These activities spurred Pres. Barack Obama to declare a national emergency in April 2015.<sup>25</sup> As the nation faces this emergency militarily, speed and depth of capabilities to defend the nation remain largely undeveloped and untested.

One might argue that this national emergency presents America with an “unrestricted battlespace” where the military can develop, test, and refine theories, weapons, and tactics of cyberpower. After all, it would appear that the US government and private sector are constantly interacting with adversaries in the domain, and thus, the military has plenty of opportunities to refine the tactics and strategies in a way that was not possible in the air domain. However, the current skirmishes in cyberspace occur during peacetime that is not unrestricted. Being prepared to advance the “use of force” or “armed conflict” levels if necessary is not the same as testing them in an operational environment against a dynamic adversary. As an example, Stuxnet only introduced us to the fringes of what is possible. As bestselling author and cybersecurity researcher Peter Singer puts it,



Yet for all the ways it could change how we engage in military operations, cyberwarfare's greatest legacy may not be any single capability or function. More likely, it will be how this new form of engagement mixes with other battlefield technologies and tactics to create something unexpected. The airplane, tank, and radio all appeared during World War I, but it wasn't until the Germans brought them together into the devastating blitzkrieg in the next global conflict that they made their lasting mark.<sup>26</sup>

Again, Stavridis and Weinstein contrast this as the "beach at Kitty Hawk" with respect to the first powered, controlled, and sustained heavier-than-air human flights by the Wright brothers in December 1903. Few, if any, could have forecasted four decades later a nation would lay in both physical and political ruin primarily as the result of the weaponized evolution and employment of the air domain. That evolution did not come easy as it covered two world wars, countless billions of dollars of investment, and incredible losses of life. Put another way, the utility and lethality of the airplane of the mid-twentieth century existed because of the merger of resources, science and technology, courage, and experience underpinned by the political will to push its capabilities through an unrestricted battlespace. This is not unique to the air domain, and one can draw similar analogies to the sea and land domains. Examples include the aircraft carrier, submarine, tank, rifle, and the forces organized, trained, and equipped to operate them. All earned their places in America's arsenal through the crucible of war.

Enduring forces, technologies, tactics, techniques, and procedures in the cyberspace domain have to travel a similar path. The difference between cyberspace and the other domains resides with the direct access to a nation's cities and its people who rely on and share the same infrastructure as military forces. Again, looking to Singer, "By the end of World War II, all sides were engaging in strategic bombing against the broader populace, arguing that the best way to end the war was to drive home its costs to civilians. As cyberwarfare becomes a reality, the same grim calculus will likely hold true."<sup>27</sup> This calculus reflects political will more than technological advancement, although each requires the other. When the political will to strike a nation's centers of gravity through cyberspace emerges, so, too, will the reality of its strategic effects and weaponry and with it the competency to engage in an informed dialogue on how best to man, train, and equip US cyberspace forces. Ultimately, much like airpower, cyberpower will not achieve rapid and unrestrained growth without the existing security competition among great

powers leading to total war. It is there where concepts and ideas thought of during peacetime are tried and tested in practice. Until then, the true effects of a separate cyber force will remain as controversial as Douhet's and Mitchell's prophecies during the interwar years. Emotions will play a significant part in the conversation, and the need for a separate cyberspace force will not extend beyond the abilities of the services and agencies to meet US national interests and objectives.

At some point each service will have to divest and return focus on core missions with cyberspace merely as a medium and not the focus of the mission. As each service dedicates resources and is shifting toward cyber operations, it creates a tension within the core competencies. This could translate into strategic cyber thought, but it then becomes more and more divorced from each service's favorite means even as it converges on their theoretical ends (for the USAF, striking at strategically important targets without having to go through the terrain- and physical-based slog to get there). Within Gen Welsh's vision of cyberpower, the USAF would have to devote resources toward "strategic strike" that may not even employ airpower. The resourcing and advocacy for this may be present in the USAF, the other services, or developed and expressed by USCYBERCOM. While it may require a separate cyber force to fulfill that vision, the time for a separate service remains premature.

## **Political Champions**

Assuming there exists a unique strategic capability in cyberspace with equivalent technologies proven in unrestricted warfare, the emergence of a separate force still requires leadership to maneuver the political and bureaucratic terrain. Because of the many actors and processes that shape force structure decisions, political champions are necessary both inside and outside the military establishment. In what David Sorenson, professor of international security studies at the Air War College, classifies as the national interest paradigm, choices about military force levels "stem from strategic assessments guided by a combination of national interests and international threats to such interests." Ultimately, competing priorities shape military investment decisions.<sup>28</sup> Simply stated, resources are finite, competition for them is intense, and compromises matter.

General Mitchell's quest for a separate USAF following World War I is one precedent in creating a new armed service when technology and operational need required it. However, the rapid pace of change in cyberspace

has not allowed time for cyberspace leaders to emerge on par with the skills and leadership qualities of General Arnold. Arnold, who trained with the Wright brothers, was a strong advocate of the airplane, evolved airpower theory through practice, and dabbled in the private sector by founding Pan American airlines.<sup>29</sup> During the interwar period, there was a 20-year gap in which leaders such as Arnold, Mitchell, and General Carl “Tooe” Spaatz could develop their technological and leadership skills. Cyberspace does not have such leadership that has been cultivated within the cyberspace career fields and resourced to experiment with tools and techniques, design operations, war game, and think about cyberspace in the upper operational and strategic levels of warfare.

Generals Marshall and Arnold fully understood the nation’s political and bureaucratic environment. With the advocacy of presidents Roosevelt and Truman, these two generals transformed an air force consisting of just over 1,200 mostly obsolete aircraft in the Army’s smallest combat arms branch at the outset of World War II into its largest and most-technologically advanced branch by the end of the war—a first in American military history.<sup>30</sup> Along the way they created an equal status of the air arm with the publishing of the War Department Field Manual 100-20, *Command and Employment of Air Power*, and gained a seat at the table in the Joint Chiefs of Staff for Arnold, the nation’s top Airman.<sup>31</sup> But it did not come at the expense of the other forces, as Marshall was keen on building a balanced force. While building the US Army Air Forces (USAAF), he also built the largest Army in US history and reorganized the Department of War from the “fiefdoms of the chiefs of infantry, cavalry, field artillery, and coast artillery” into the three commands: the army Ground Forces, the Services of Supply, and the USAAF.<sup>32</sup> The reorganization provided the USAAF with “sufficient clout to move their requirements with dispatch through the War Department General Staff.”<sup>33</sup>

While building the USAAF, Marshall and Arnold had to “continually fend off congressional demands on the question of an independent air force,” a trend originated in the interwar years that gained additional traction during the war. With an eye to the future, the generals successfully deferred the discussion until after the war and concentrated on victory and building the legitimacy of airpower and the nucleus of Airmen needed to sustain it.<sup>34</sup> As previously noted, this included the high-risk development of the B-29, the autonomous standup of the Twentieth Air Force, and the fusion of the bomber and the atomic bomb that

pushed the world into the nuclear age. The underlying goal was not just air force independence but also to establish a USAF in the postwar national security reorganization that allowed for its own budget and to seamlessly fit into a “coordinated organization of ground, air, and naval forces in operational theaters, each under its own commander, and each responsible to a supreme commander.”<sup>35</sup> The push for a unified, integrated defense establishment, supported by President Truman, General Eisenhower, and many others, became part of the National Security Act of 1947 that established the National Military Establishment, secretary of defense, Joint Chiefs of Staff, the National Security Council, and the Central Intelligence Agency in addition to the USAF.<sup>36</sup> Air force independence was established, but in the context of much larger national security changes to deal with the postwar world order.

With the exception of Admiral Stavridis, there do not appear to be many leaders—military, congressional, or otherwise—backing the formation of an independent US cyber force at this time. Most observers agree the United States is dangerously vulnerable in cyberspace, but they do not look at it as a purely military problem that a separate force could solve. Throughout 2015, numerous influential congressional, government, military, and industry leaders presented multiple differing views on the threats posed by nations and actors in cyberspace. Internationally, nations worldwide are pushing their own plans to organize, train, and equip for cyberwarfare. As one article succinctly puts it, “Countries toiled for years and spent billions of dollars to build elaborate facilities that would allow them to join the exclusive club of nations that possessed nuclear weapons. Getting into the cyberweapon [*sic*] club is easier, cheaper and available to almost anyone with cash and a computer.”<sup>37</sup> Despite this threat, the call for a separate US cyber force is nearly nonexistent. This does not prove one is not needed. Merely, it speaks to the lack of political champions for such change to the military establishment.

### **Time for a Cyber Agency**

Without a doubt, the nation faces a national emergency in cyberspace, and something must be done. Indeed, it may require not a new armed service, but a new act of Congress reordering the national security apparatus. From a military perspective, the standup of the USCYBERCOM as a subordinate unified command under US Strategic Command (USSTRATCOM) seems to satisfy the current appetite for restructuring.

Looking to the future, the next logical step toward a cyber force, as Stavridis points out, is a modification to the Unified Command Plan raising USCYBERCOM to full combatant command status. In fact, it is a question the Senate Armed Services Committee asked Adm Michael Rogers, current commander of USCYBERCOM, as part of his confirmation process in March 2014.<sup>38</sup> The question was, “What are the best arguments for and against taking such action now?” Admiral Rogers replied there were no impediments to an elevation in status other than an increase in staff to accomplish “administrative functions” such as budgeting and force management at that level. As for the benefits, Rogers stated, “Elevation to full unified status would improve resource advocacy, allocation and execution by improving input to Department [DOD] processes and eliminating competition in prioritization. Additionally, alignment of responsibility, authority, situational awareness, and capability under a single commander would improve cyberspace operations and planning.”<sup>39</sup>

In an act of patriotism, Stavridis and Weinstein proposed a solution they deemed necessary to contend with the current threat environment. The current malicious activities in cyberspace should be evidence enough that warfare in cyberspace, unhindered, will occur, and the United States should take action now to begin the organizational processes to prepare for combat. However, a cyber force is currently the wrong construct through which America assures its national security and economic interests. Competition in cyberspace today is characterized by international interaction where states and nonstate actors compete with each other in direct contact that is often short of armed conflict and only ambiguously within the framework of use of force. Military advocacy has been to “open up” or “expand” the scope of what fits into a “legitimate use of military capabilities” framework. For many others, both interagency and internationally, this militarizes cyberspace and generates consternation. Therefore, as a nation, we must think deeply about what cyber operations should be able to accomplish in pursuit of our national interests and protecting our values, not just in war but in peacetime. A broader restructuring of the US national security apparatus is necessary to counter the threat.

Within a new national security framework for cyberspace, a cyberspace agency could be created and modelled after the National Oceanic and Atmospheric Administration, the Public Health Service, or the Coast Guard rather than the Army, Navy/Marines, or USAF. This should not

hinder the evolution of the capabilities within the services, but it should develop within the context of enhancing their missions much like the aircraft carrier in the Navy and rotary-wing operations in the Army. Neither changed the fundamental need for strategic bombing nor the tactical enhancements airpower provided existing core service functions. It would thus be a uniformed and even armed service in the sense that it is designed to operate across both civilian and military mission spaces, likely with some level of counterintelligence and even law enforcement authorities and in close cooperation with the private sector. Thinking through and optimally designing this structure is a wicked problem.


## **Conclusion**

Without question, the United States faces unprecedented threats in cyberspace while the military services and combat-support agencies continue to feel their way around the terrain, developing both offensive and defensive capacity. Because of these threats and the uneasiness that comes with them requests for changes in the military force structure have surfaced, including Stavridis's and Weinstein's calls for a US cyber force independent of the other services. The basis of their argument is that the United States traveled a similar path in creating an independent air force, citing General Mitchell's crusade following World War I as an historical precedent. However, a better framework to assess whether the threats warrant a separate US cyber force is to analyze the key criteria reached by the USAAF during World War II that persuaded legislators, military leaders, and the American public to establish an independent air force. Specifically, these criteria are a unique, strategic military capability; equivalent technological advances; an unrestricted battlespace; and political champions to maneuver the bureaucratic and legislative terrain.

Using the USAF's path to independence as a basis, an analysis of cyberspace force capabilities reveals that the services and combat-support agencies can meet current strategic national requirements. Technological advances remain tactical and secretive. Though contested, cyberspace is still bounded by reality and has not evolved to an unrestricted battlespace. And political champions calling for a separate US cyber force are scarce at the present time. Even with developments of the strategic bombing theories, the advent of long-range bombers, World War II, and top US leaders who backed a separate air force, competing visions and interservice maneuvering won the day by dividing responsibilities for

the air domain among each of the combatant arms. The emergence of a separate cyber force may be as difficult, with an additional challenge. In strategic air warfare, much of the required technology was embodied in the airplanes and bombs, while in cyber warfare, the experiential requirements of highly educated and trained personnel may prove the principal mobilization concern. Cyberspace is fundamentally different from the physical domains in that it is more about outthinking an adversary. This is a new paradigm in that we are only at risk to the extent we allow logic to exploit our unknown cyber insecurities and potentially create effects.

Unfortunately, the criteria presented here will likely not be reached until after the first overt, nation-state war that extensively includes cyberspace. Much like World War II, this future war will look different than anything seen to date but will surely be won by the nations that can control cyberspace in a way the Allies controlled the skies in Europe and the Pacific. Debates and hypothetical conjectures about the potential effects of cyber as a source of vulnerability or as an aspect of national power will continue. A restructuring of the US national security apparatus is necessary to operationalize cyberspace for the purposes of projecting national power, defending our critical infrastructure and key resources, developing and testing tactics and techniques for war and countermeasures short of war, and thinking about deterring others from doing the same to us. While the technological advances will likely lag, ultimately, nothing shapes and evolves military capabilities like war. Just as in 1947, any discussion of a separate cyber force should not be separated from discussions of how to optimize the design of the entire national security establishment to pursue national interests in the new domain. Indeed, it took the complete alteration of the US national security structure to create the USAF in 1947. Without a cogent understanding of cyberpower and the dynamics of conflict in the domain, we cannot say for sure that a separate armed service will best be focused on combat, as opposed to fulfilling national objectives up to and including, but not limited to, combat. Stavridis's reference to the "beach at Kitty Hawk" highlights the infancy of lucid strategic thinking about cyberspace outside of the niche cyber-warfare community. There has been an almost 30-year heritage of cyber operations that has failed to synthesize a coherent theory of cyberpower in pursuit of national interests.<sup>40</sup> The time between the creation of the US Army Air Corps in 1926 and the end of World War II framed

the airpower debate, tested its major concepts and theories, developed distinct air domain technologies, and set the conditions for a separate air force to further US development and exploitation of the air domain. Three decades of discussion about a domain that is largely invisible and cognitive has failed to provide a strategic context within which to analyze the touchstones necessary to sway lawmakers, military leaders, and the American public to the idea of a separate force to pursue US national interests in cyberspace. 

## Notes

1. Joint Publication 3-12 (R), *Cyberspace Operations*, 5 February 2013, I-1. The definition of cyberspace as published in joint doctrine states cyberspace is “the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (v). It further explains cyberspace in terms of three layers: physical network, logical network, and cyber-persona. For the purposes of this article, this is the definition that will be used to assess and analyze the merits and challenges of establishing a separate US cyber force. However, the authors contend cyberspace (as defined here) is in fact not the domain but rather the tools and platforms used to operate within the electromagnetic spectrum. Cyber and electronic warfare are both converging, and this convergence must be appreciated; however, it is beyond the scope of this article to discuss the convergence of the two as operational domains of conflict. We focus solely on the doctrinal cyberspace, while encouraging the cyber/electronic-warfare communities to consider their interrelationships and dependencies in further discussions of creating on cyber force.

2. This is not a new discussion. Indeed, many point to the same question about a US space force and the previous three decades of debate on the topic. Our intent here is to address one analogy and not all possible analogies connected to the creation of separate armed services for domains. Briefly, the difference is that in space, strategic effects on targets cannot be made. This also represents a reflection of the fact the United States has not experienced an unrestricted battlespace in either domain where political will unleashed all capabilities to confront an adversary.

3. James Stavridis and David Weinstein, “Time for a U.S. Cyber Force,” *Proceedings* 140, no. 1 (January 2014), <http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force>, accessed 15 October 2014.

4. *Ibid.*

5. Senate, Testimony of Admiral James Stavridis, USN (Ret) before the Senate Armed Services Committee, 114th Cong., 1st sess., 10 December 2015, [http://www.armed-services.senate.gov/imo/media/doc/Stavridis\\_12-10-15.pdf](http://www.armed-services.senate.gov/imo/media/doc/Stavridis_12-10-15.pdf).

6. Ian Duncan, “Defense Secretary: We Could Create Separate Military Force to Fight Cyber Wars,” *Baltimore Sun*, 13 March 2015, <http://www.baltimoresun.com/news/maryland/bal-defense-secretary-we-could-create-separate-service-to-fight-cyber-wars-20150313-story.html>.

7. Herman S. Wolk, *Reflections on Air Force Independence* (Washington, DC: Air Force History and Museums Program, 2007), 55.



8. Ibid., 67–68.
9. Mark Welsh III, “Air Force Update” (speech, Air Force Association’s Air & Space Conference and Technology Exposition, 16 September 2014), <http://www.af.mil/Portals/1/documents/af%20events/Speeches/16SEP2014-CSAF-GenMarkWelsh-AFUpdate.pdf?timestamp=1410982866264>.
10. David MacIsaac, “Voices from the Central Blue: The Air Power Theories,” in *Makers of Modern Society from Machiavelli to the Nuclear Age*, edited by Peter Paret (Princeton, NJ: Princeton University Press, 1986), 624–47.
11. Ibid., 626.
12. Ibid., 631.
13. Department of Defense, *Quadrennial Defense Review 2014* (Washington, DC: DOD, 2014), 41, [http://www.defense.gov/pubs/2014\\_Quadrennial\\_Defense\\_Review.pdf](http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf).
14. Wolk, *Reflections on Air Force Independence*, 45, 59.
15. Ibid., 48–49.
16. Thomas H. Coffey, *Hap: The Story of the US Air Force and the Man Who Built It* (New York: The Viking Press, 1982), 374.
17. Ibid.
18. Richard B. Frank, *Downfall: The End of the Imperial Japanese Empire* (New York: Penguin, 1999), 334.
19. Harry S. Truman, *Memoirs*, vol. 2, *Years of Trial and Hope* (Garden City, NY: Doubleday and Co., Inc., 1956), 46.
20. Eric P. Oliver, “A Case Study in Cyber Warfare,” in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, edited by Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton, FL: Taylor & Francis, 2013), 127–60.
21. Kennette Benedict, “Stuxnet and the Bomb,” *Bulletin of the Atomic Scientists*, 15 June 2012, <http://thebulletin.org/stuxnet-and-bomb>.
22. Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve* (Arlington, TX: Langner Group, November 2013), 10, <http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.
23. Ibid., 15.
24. Barack Obama, “Statement by the President on Executive Order ‘Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,’” (press release, Office of the Press Secretary, 2 April 2015), <https://www.whitehouse.gov/the-press-office/2015/04/02/statement-president-executive-order-blocking-property-certain-persons-en>.
25. Exec. Order No. 13694 (1 April 2015), <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.
26. Peter W. Singer, “The War of Zeros and Ones,” *Popular Science*, 8 September 2014, <http://www.popsoci.com/article/technology/war-zeros-and-ones>.
27. Ibid.
28. David S. Sorenson, *The Process and Politics of Defense Acquisition: A Reference Book* (Westport, CT: Praeger Publishers, 2009), 90.
29. Bill Yenne, *Hap Arnold: The General Who Invented the US Air Force* (Washington, DC: Regnery History, 2013), 51.
30. Wolk, *Reflections on Air Force Independence*, 3.
31. Ibid., 30; and Coffey, *Hap: The Story of the US Air Force*, 259.
32. Ed Cray, *General of the Army: George C. Marshall, Soldier and Statesman* (New York: W.W. Norton and Company, 1990), 279.
33. Wolk, *Reflections on Air Force Independence*, 27.

34. Ibid.
35. Ibid., 78.
36. Ibid., 96–97.
37. Damian Paletta, Danny Yadron, and Jennifer Valentino-Devries “Cyberwar Ignites New Arms Race,” *Wall Street Journal*, 12 October 2015, A-1, <http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128>.
38. Senate Armed Services Committee, “Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command,” 11 March 2014, 29–30, [http://www.armed-services.senate.gov/imo/media/doc/Rogers\\_03-11-14.pdf](http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf).
39. Ibid.
40. Jason Healey, “Claiming the Lost Cyber Heritage,” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 11–19, <http://www.au.af.mil/au/ssq/2012/fall/healey.pdf>.

### **Disclaimer**

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: [strategicstudiesquarterly@us.af.mil](mailto:strategicstudiesquarterly@us.af.mil).